Diese Website verwendet Cookies von Google, um Dienste anzubieten und den Traffic zu analysieren. Deine IP-Adresse und dein User-Agent werden zusammen mit Messwerten zur Leistung und Sicherheit für Google freigegeben. So können Nutzungsstatistiken generiert, Missbrauchsfälle erkannt und behoben und die Qualität des Dienstes gewährleistet werden.

WEITERE INFORMATIONEN OK

Saturday, January 31, 2009

Confidential auditing

I once described how confidential auditing was possible and beneficial:

> The auditing function is a vast and indispensable part of the modern economy. Auditing controls allow, among other things, employers to delegate resources and authority to employees, franchisors to delegate to franchisees, stockholders to delegate to management, advertisers to count eybeballs, marketers to gather more reliable data on customers, and make possible a wide variety of other such relationships. Auditing controls might fairly be called the security protocols of capitalism...[However,] auditing is in deep conflict with efforts towards greater privacy. Auditors have an ethic of recording, investigating, and reporting as much as possible, and often see privacy efforts as attempts to prevent auditing and potentially cover up fraud...[But confidential auditing is possible because] we can achieve auditing logs unforgeable after commitment via secure timestamps. We can then achieve to a great extent unforgeability prior to commitment, with segregation of duties via multiparty integrity constraints. We then audit these commitments via multiparty private computations.

In an article about multiparty secure (i.e. private) computations I described this process as follows:

> Performance phase analysis with multiparty secure computer theory would seem to apply only to those contracts which can be performed inside the virtual computer. But the use of post-unforgeable auditing logs, combined with running auditing protocols inside the shared virtual computer, allows a wide variety of performances outside the virtual computer to at least be observed and verified by selected arbitrators, albeit not proactively self-enforced.
>
> The participants in this mutually confidential auditing protocol can verify that the books match the details of transactions stored in a previously committed transaction log, and that the numbers add up correctly. The participants can compute summary statistics on their confidentially shared transaction logs, including cross-checking of the logs against counterparties to a transaction, without revealing those logs. They only learn what can be inferred from the statistics; [they] can't see the details of the transactions

In this I had been inspired by Eric Hughes' idea of encrypted open books. My sketch is more general insofar as it addresses pre-transaction forging (with separation of duties), post-transaction forging (with secure timestamping), and the auditing protocol itself (with multiparty private computation running off the logs themselves rather than Hughes' specialized protocol running off already

Pages

- Home

About Me

Nick Szabo

"A premier thinker about history, law and economics, and the lessons they have for security." -- Adam Shostack, Emergent Chaos

"Szabo comes out with these essays that leave me in awe." -- Brian Dunbar

"Reading material that is eclectic, challenging and endlessly fascinating." -- Sean McGrath, Propylon

"Like most blogs worth my attention, this blog is updated only infrequently. That is because the authors of blogs worth my attention only post when they have something to say that is true, relevant and not already known by their audience. Most of the human race does not have the skill to know when an idea has these three properties. The skill is particularly rare in the fields of politics and economics, which is why this blog is such a rare and valuable thing." -- Richard Hollerith

View my complete profile

prepared books).

But my description was only a proof-of-concept sketch that one could go all the way from preparing to transact to transaction log to finished audits while maintaining both integrity and privacy, with neither depending on large amounts of trust in the auditors. Recently Shen et. al. came up with a detailed design of such a confidential auditing scheme in the context of gathering statistics from the logs of distributed computations:

> ...no single TTP [trusted third party] node can have the full knowledge of the logs, and thus no single node can misuse the log information without being detected. On the basis of a relaxed form of secure distributed computing paragidms, one can implement confidential auditing service so that the auditor can retrieve certain aggregated system information e.g., the number of transactions, the total volume, the event traces, etc., without having to access the full log data...To prevent an unsupervised TTP from manipulating the system, we design query processing schemes that require TTP nodes work together, using the multiparty private computation, to perform any useful auditing functions.

Posted by Nick Szabo at 5:36 PM

6 comments:

Michel said...

Dear Nick Szabo,

I am a contributor to the German Wikipedia. My main project is an article about free banking, which I want to illustrate by some pictures of your blog on the site:
http://unenumerated.blogspot.com/2008/05/bank-notes-from-free-banking-era.html
In order to do so I want to load them up in wiki commons. We don't have to deal with copyright stuff, because the originals are so old and as non-creative acts, photographing cannot create any new copyright. See

http://commons.wikimedia.org/wiki/Commons:When_to_use_the_PD-scan_tag

and

http://en.wikipedia.org/wiki/Wikipedia:PD

for more information. Please tell me if I am wrong (e.g. you used a lot of creativity to enhance the photos). If you don't object, I will put a link to your side and mention that you have made the photos in the description.

Kindly regards,
Robert Michel

12:59 PM

Michel said...

And by the way nice blog!

Blog Archive

- 2018 (1)
- 2017 (3)
- 2016 (4)
- 2015 (3)
- 2014 (3)
- 2013 (3)
- 2012 (8)
- 2011 (12)
- 2010 (9)
- 2009 (29)
  - November (3)
  - October (6)
  - September (3)
  - August (1)
  - July (1)
  - June (3)
  - May (6)
  - April (3)
  - January (3)
    - Law embedded in the world
    - Confidential auditing
    - Secure timestamping and confidential auditing
- 2008 (55)
- 2007 (47)
- 2006 (130)
- 2005 (44)

1:00 PM

nick said...

These are indeed my photos and you have my permission to copy and distribute them on Wikipedia, and I welcome your link(s).

best wishes,
Nick Szabo

5:16 PM

Michel said...

Thank you, it seems the photofiles contain some information about your camera, you may have a look at them.

7:36 AM

Michel said...

link = http://commons.wikimedia.org/wiki/Category:US_Free_Banking_Era_banknotes

7:38 AM

gwern said...

Final paper link is broken; IA has it at
http://web.archive.org/web/20070418003710/http://faculty.cs.tamu.edu/zhao/papers/conf/2004/0403-ICDCS-SLLZ.pdf

2:09 PM

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

Simple theme. Powered by Blogger.